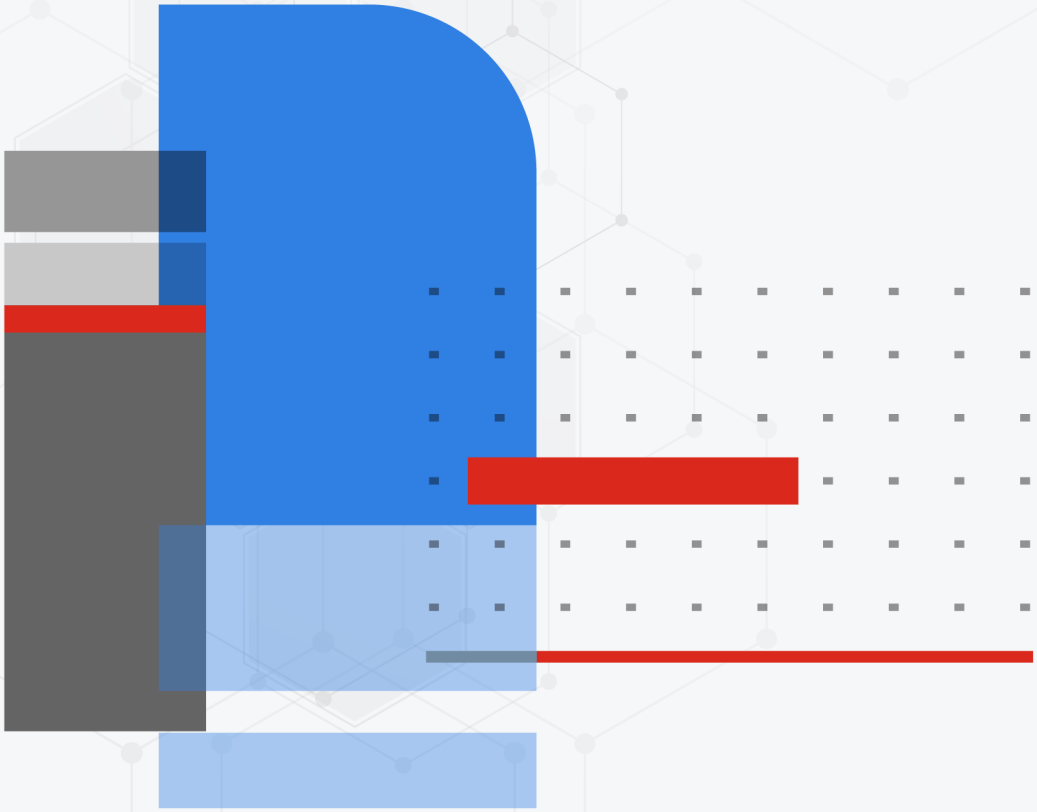
Release Notes

FortiAnalyzer Cloud 7.6.7 R1



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

June 9, 2026
FortiAnalyzer Cloud 7.6.7 R1 Release Notes
05-767-1298904-20260609

TABLE OF CONTENTS

Change log

Date	Change Description
2026-06-09	Initial release.

FortiAnalyzer Cloud 7.6.7 R1 release

This document provides information about FortiAnalyzer Cloud version 7.6.7 R1 build 3737 (KVM build 3737 and K8S build 6183).

The recommended minimum screen resolution for the FortiAnalyzer Cloud GUI is 1920 x 1080. Please adjust the screen resolution accordingly. Otherwise, the GUI may not display properly.

Special notices

This section highlights some of the operational changes that administrators should be aware of in FortiAnalyzer Cloud version 7.6.7 R1.

FortiClient logging

When configuring logging from FortiClient to FortiAnalyzer Cloud, you must manually enter the fully qualified domain name (FQDN) of the FortiAnalyzer Cloud instance in the *IP Address/Hostname* field. It is important that this information is entered accurately to ensure your data is sent to the correct FortiAnalyzer Cloud instance.

For more information on configuring FortiClient logging to FortiAnalyzer Cloud, see the FortiClient documentation on the Fortinet Docs Library.

Upgrade information

A notification is displayed in the FortiAnalyzer Cloud notification drawer when a new version of the firmware is available. You can chose to upgrade immediately or schedule the upgrade for a later date.

In FortiAnalyzer Cloud 7.4.3 and later, administrators must perform firmware upgrades from within the FortiAnalyzer Cloud Dashboard or firmware upgrade notification drawer.

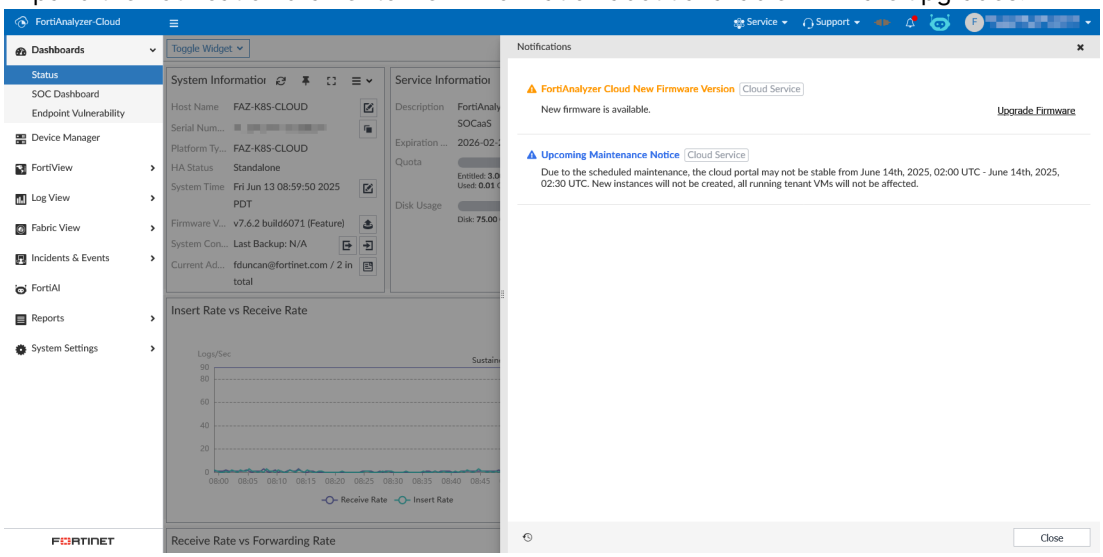
An administrator with Super_User permissions is required to perform the upgrade.

To keep FortiAnalyzer Cloud secure and up to date, it is recommended that you upgrade your 7.6 release to the latest release build.

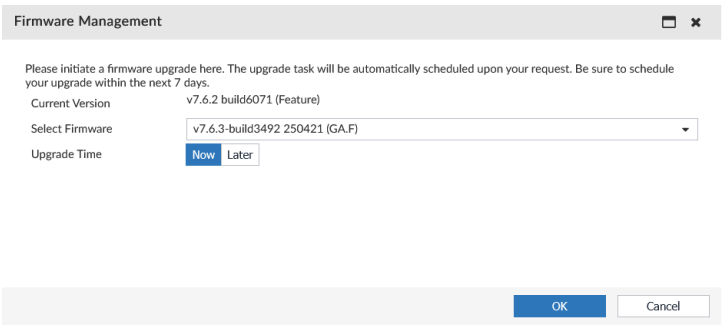
An email will be sent to notify you when an upgrade is mandatory. After receiving the notification, you will have 14 days to complete the upgrade. See Mandatory upgrades on page 9.

To upgrade firmware from the notification drawer:

1. Go to FortiAnalyzer Cloud (https://fortianalyzer.forticloud.com/), and use your FortiCloud account credentials to log in. An administrator with Super_User permissions is required to perform the upgrade.
2. Expand the notification drawer to view information about available firmware upgrades.



3. Click *Upgrade Firmware* to update the firmware immediately or to schedule upgrade of the firmware for a later date.



4. Click *OK* to perform or schedule the upgrade.

To upgrade firmware from the Dashboard:

1. Log in to your FortiAnalyzer Cloud instance.
2. Go to *Dashboard* in the tree menu.
3. In the *System Information* widget, select the upgrade icon next to the firmware version.
   The *Firmware Management* dialog appears. The current firmware version is displayed along with upgrade options.
4. In the *Select Firmware* field, choose an available firmware version.
5. In the *Upgrade Time* choose *Now* or *Later*.
   - *Now*: Begin the upgrade immediately.
   - *Later*: Schedule the upgrade for a later time.
6. Click *OK*. The upgrade will be completed based on the selected options.

FortiAnalyzer Cloud upgrade path

When upgrading FortiAnalyzer Cloud between major/minor versions, you must first upgrade to the latest patch release for the current version and any intermediate versions.

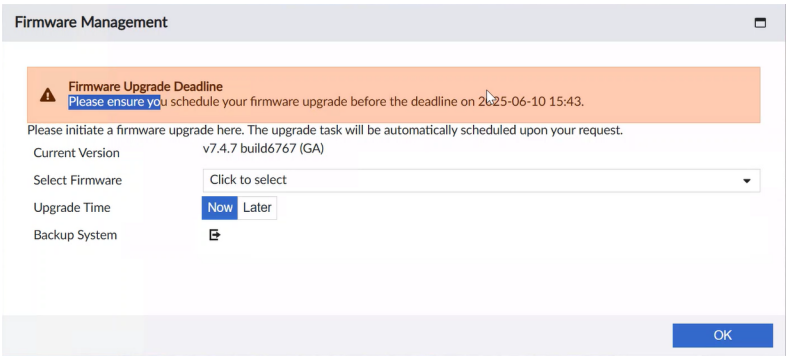
For example, in order to upgrade FortiAnalyzer Cloud from version 7.2.x to 7.6.x, you must first upgrade to the latest 7.2 patch version, followed by the latest 7.4 patch version, before finally upgrading to the target 7.6.x release.

The FortiAnalyzer Cloud firmware version selection menu only displays the next eligible version that your instance can be upgraded to in the path. In the example above, the 7.4 firmware would not be displayed as an option until you have updated to the latest available 7.2 patch version.

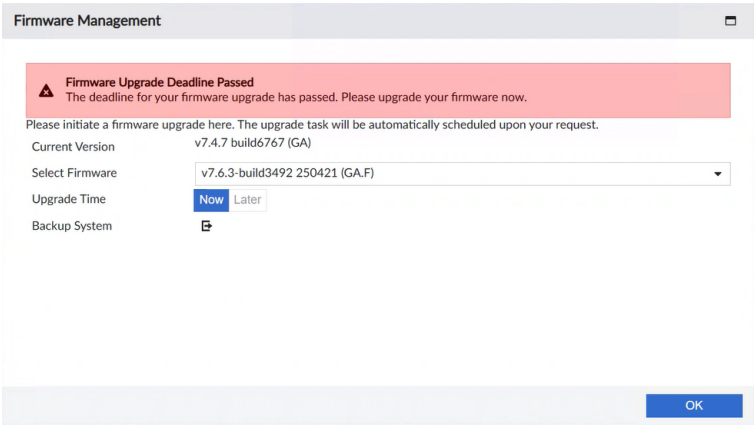
Mandatory upgrades

When a firmware upgrade is mandatory, a *Firmware Management* dialog window will appear when you access your instance. This dialog provides details about the upgrade deadline and options for upgrading your firmware

version. You can choose to upgrade immediately or schedule the upgrade for a later time. This dialog cannot be bypassed.



After the deadline has passed, you can still connect to your instance's GUI to see the *Firmware Management* dialog window, however, you will only have the option to upgrade immediately. This dialog cannot be bypassed and you will not be able to access your instance until the upgrade is completed.



Downgrading to previous versions

Downgrade to previous versions of FortiAnalyzer Cloud firmware is not supported.

Product integration and support

This section lists FortiAnalyzer Cloud 7.6.7 R1 support of other Fortinet products. It also identifies what FortiAnalyzer Cloud features are supported for log devices and what languages FortiAnalyzer Cloud GUI and reports support.

The section contains the following topics:

Software support

FortiAnalyzer Cloud 7.6.7 R1 supports the following software:

Web browser support

FortiAnalyzer Cloud version 7.6.7 R1 supports the following web browsers:

- Microsoft Edge 114
- Mozilla Firefox version 96
- Google Chrome version 114

Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS support

FortiAnalyzer Cloud version 7.6.7 R1 supports the following FortiOS versions:

See the FortiAnalyzer 7.6.7 Release Notes for the latest supported FortiOS versions.

- 7.6.0 and later.
- 7.4.0 and later
- 7.2.0 and later

FortiClient support

FortiAnalyzer Cloud version 7.6.7 R1 supports the following FortiClient versions:

See the FortiAnalyzer 7.6.7 Release Notes for the latest supported FortiClient 7.0 versions.

- 7.4.0 and later
- 7.2.0 and later
- 7.0.3 and later

FortiEndpoint support

FortiAnalyzer Cloud version 7.6.7 R1 supports FortiEndpoint.

FortiMail support

FortiAnalyzer Cloud version 7.6.7 R1 supports the following FortiMail versions:

See the FortiAnalyzer 7.6.7 Release Notes for the latest supported FortiMail versions.

- 7.6.0 and later
- 7.4.0 and later
- 7.2.0 and later

FortiWeb support

FortiAnalyzer Cloud version 7.6.7 R1 supports the following FortiWeb versions:

See the FortiAnalyzer 7.6.7 Release Notes for the latest supported FortiMail versions.

- 7.6.0 and later
- 7.4.0 and later
- 7.2.0 and later
- 7.0.0 and later

FortiNDR support

FortiAnalyzer Cloud version 7.6.7 R1 supports the following FortiNDR versions:

- 7.6.3 and later

FortiSandbox

FortiAnalyzer Cloud version 7.6.7 R1 supports the following FortiSandbox versions:

- FortiSandbox 5.0.3 and later

Feature support

FortiAnalyzer Cloud version 7.6.7 R1 provides the following feature support:

Platform	Log View	FortiView	Event Management	Reports
FortiGate	✓	✓	✓	✓
FortiClient EMS	✓	✓	✓	✓
FortiEndpoint	✓	✓	✓	✓
FortiMail	✓	✓	✓	✓
FortiWeb	✓	✓	✓	✓
FortiNDR	✓	✓	✓	✓
FortiSandbox	✓		✓	✓

Language support

The following table lists FortiAnalyzer Cloud language support information.

Language	GUI	Reports
English	✓	✓
Chinese (Simplified)	✓	✓
Chinese (Traditional)	✓	✓
French	✓	✓
Hebrew		✓
Hungarian		✓

Language	GUI	Reports
Japanese	✓	✓
Korean	✓	✓
Russian		✓
Spanish	✓	✓

To change the FortiAnalyzer Cloud language setting, go to *System Settings* > *Admin* > *Admin Settings*, in *Administrative Settings* > *Language* select the desired language from the drop-down list. The default value is *Auto Detect*.

Russian, Hebrew, and Hungarian are not included in the default report languages. You can create your own language translation files for these languages by exporting a predefined language from FortiAnalyzer Cloud, modifying the text to a different language, saving the file as a different language name, and then importing the file into FortiAnalyzer Cloud. For more information, see the *FortiAnalyzer Administration Guide*.

Model support

FortiAnalyzer Cloud supports the same FortiGate, FortiMail, and FortiWeb models as FortiAnalyzer 7.6.7. For a list of supported models, see the *FortiAnalyzer 7.6.7 Release Notes* on the Document Library.

Resolved issues

The following issues have been fixed in FortiAnalyzer Cloud version 7.6.7 R1. To inquire about a particular bug, please contact Customer Service & Support.

Event Management

Bug ID	Description
1275382	The webhook for the event handler is still being triggered even though it was already suppressed.

Log View

Bug ID	Description
1198027	No results are returned when filtering the Event Message column by a suggested value that contains a comma.

Others

Bug ID	Description
1282570	Changing system time on K8S will affect time in other instances on the same node.
1284886	When user adds 1000+ seats -463- license, Entitled Quota shows only 1 GB/day
1273761	EMS cloud connector failed to run "Get Vulnerabilities" playbook.

Reports

Bug ID	Description
1224929	Following the upgrade, the data shown in the VPN reports Top 5 Site-to-Site IPsec Tunnels by Bandwidth chart appears to be inaccurate.

System Settings

Bug ID	Description
1128305	The forwarding rate is not zero when the log forwarding server is disabled or not configured.

Known issues

Known issues are organized into the following categories:

- New known issues
- Existing known issues

To inquire about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

New known issues

No new issues have been identified in version 7.6.7 R1.

Existing known issues

The following issues have been identified in a previous version of FortiAnalyzer Cloud and remain in FortiAnalyzer Cloud 7.6.7 R1.

Fabric View

Bug ID	Description
1231421	Playbook fail to run for downstream FortiGates in Security Fabric.
1236262	FortiOS Connector does not appear under the correct Security Fabric name.

FortiSoC

Bug ID	Description
1202951	Outbreak Alerts page displays the report list is unavailable in FortiGuard despite valid license and connectivity.

FortiView

Bug ID	Description
1092311	FortiAnalyzer may not display any data when accessing FortiView in the VPN site-to-site tab.

Others

Bug ID	Description
1098690	After an upgrade, users (prior to the upgrade) who were created and assigned to a custom admin profile (with the super_user_profile enabled) may encounter a GUI issue. Upon successful login, the login prompt disappears, but only the background color remains visible, with no additional GUI elements loaded.

Reports

Bug ID	Description
1127015	FortiAnalyzer report charts are shifted if Print Orientation is set to "Portrait".

System Settings

Bug ID	Description
1142016	The *Index Fetched Logs* feature in *Request Fetch under Advanced > Log Fetch* is not functioning as expected.

Limitations of FortiAnalyzer Cloud

All FortiAnalyzer modules are supported in FortiAnalyzer Cloud; however, the following features are not supported or are not relevant to the FortiAnalyzer Cloud deployment at this time:

- Logging Topology
- ADOMs
- Advanced ADOM mode
- High-Availability Mode
- Syslog logging from third-party devices: Syslog logging from third-party devices is supported using log forwarding from an on-premise FortiAnalyzer only.
- Logging from FortiClient EMS for Chromebook
- Fetcher Management
- Remote Certificates
- The FortiAnalyzer Cloud Dashboard widget availability differs from on-premises FortiAnalyzer:
  - The License Information widget is replaced with the Service Information widget which includes differences from on-premises FortiAnalyzer. For more information, see Storage quota and disk usage on page 24.
  - FortiAnalyzer Cloud does not support the *System Resources*, *Unit Operation*, *Alert Message Console*, *Disk I/O*, and *Disk Quota Usage* widgets.
  - FortiAnalyzer Cloud includes *Historical Log Rate*, *Average Log Rate*, *Average Quota*, and *Historical Quota Usage* widgets that are not available in on-premises FortiAnalyzers.
- Remote Authentication Server
- SAML SSO
- SNMP monitoring tool
- Trusted Hosts
- Security Rating Compliance Reports
- Pre-login banners
- Remote connection to authorized devices from the Device Manager using *Connect to Device*.
- FortiAnalyzer Cloud can not be configured as Supervisor in a FortiAnalyzer Fabric.

FortiAnalyzer Cloud supports logs from FortiGate devices and non-FortiGate devices, such as FortiClient.

FortiAnalyzer Cloud can be integrated into the Cloud Security Fabric when the root FortiGate is running firmware version 6.4.4 or later.

The FortiAnalyzer Cloud portal does not support IAM user groups.

Logging support and daily log limits

The daily log limits available for FortiGate devices depend on the device platform. These daily log limits can be expanded with an additional storage license. Adding additional storage licenses also enables FortiAnalyzer Cloud to receive logs from other supported devices like FortiClient and FortiMail.

For more information on licensing and SKUs, see the FortiAnalyzer Cloud Deployment Guide and FortiAnalyzer Cloud Datasheet.

FortiGate and FortiWeb devices

FortiAnalyzer Cloud supports logs from FortiGate and FortiWeb devices. Each FortiGate or FortiWeb device with an entitlement is allowed a fixed daily rate of logging.

When determining the daily log limit for FortiAnalyzer Cloud, the form factor of the model determines the log limits. The chart below identifies some models for each form factor as an example. It is not an exhaustive list.

The following rates are based on the FortiAnalyzer Cloud a la carte subscription:

FortiGate

Form Factor	Example FortiGate Model	Total daily log limit	Rate limit quota
Desktop or FGT-VM models with 2 CPU	FortiGate 30 series, FortiGate 90 series	200MB/Day	6 logs/second
1RU or FGT-VM models with 4 CPU	FortiGate 100 series, FortiGate 600 series, FortiGate 800 series, FortiGate 900 series	1GB/Day	30 logs/second
2 RU and above or FGT-VM models with 8 CPU and above	FortiGate 1000 series and higher	5GB/Day	150 logs/second

FortiWeb

Form Factor	Example FortiWeb Model	Total daily log limit	Rate limit quota
Desktop or FWB-VM models with 2 CPU or less	FWB-100F FWB-VM (2 CPU or less)	1GB/Day	20 logs/second
1RU and above or FWB-VM models with 4 CPU or higher	FWB-400F FWB-600F FWB-1000F FWB-2000F FWB-3000F FWB-4000F FWB-VM (4 CPU or higher)	5GB/day	100 logs/second

Once the limit has been reached, users must purchase additional storage in order for FortiAnalyzer Cloud to maintain logs for 12 months. You can purchase additional storage licenses to expand the daily logging limits for your FortiGate and FortiWeb devices. For more information about daily log limits included with additional storage licenses, see Additional Storage licenses on page 23.

Additional Storage licenses

Additional storage licenses are available to expand the base daily logging limits. Multiple of the same SKU may be combined.

Added daily log limit	SKU	Rate limit quota
+5 GB/day	FC1-10-AZCLD-463-01-DD	150 logs/second
+50 GB/day	FC2-10-AZCLD-463-01-DD	1500 logs/second
+500 GB/day	FC3-10-AZCLD-463-01-DD	15000 logs/second

Daily log limits for non-FortiGate/FortiWeb devices

Purchasing any of the additional storage licenses above (for example, FC1-10-AZCLD-463-01-DD) also enables FortiAnalyzer Cloud to receive logs from FortiClient and FortiMail in addition to expanding the amount of logs it may store from FortiGates.

Storage add-on licenses

The impact of storage add-on licenses depends on whether FortiAnalyzer Cloud is receiving logs from FortiGate devices.

To see information about FortiAnalyzer Cloud licensing, see the FortiAnalyzer Cloud Deployment guide.

Storage quota and disk usage

The *Service Information* widget on the FortiAnalyzer Cloud Dashboard displays the following information:

Description	The service description.
Expiration Date	The expiration date of the license.
Quota	Quota displays the current day's storage entitlement and usage. This includes storage space used by both raw logs and database logs. Click the list icon to see a breakdown of quota usage over the past 7 days. **Quota field calculation** The *Quota* field on FortiAnalyzer Cloud differs from the *GB/Day* field and `diagnose fortilogd logvol-adom all` command in on-premise FortiAnalyzers which only shows the *raw log volume* for the last 7 days.
Disk Usage	Displays the amount of disk currently being used as well as the total available disk size.
FortiGuard	Displays the licensing status and entitlement usage of add-on services for FortiAnalyzer Cloud, including: • Security Rating Update • Industrial Security Service

Information about other Dashboard widgets shared between on-premises FortiAnalyzer and FortiAnalyzer Cloud can be found in the FortiAnalyzer Administration Guide.

Log insertion rate limits

FortiAnalyzer Cloud uses log rate limits to determine the maximum number of logs that can be inserted into its database per second.

The following are used to determine the number of logs that are supported:

Sustained log rate	The supported number of logs that FortiAnalyzer Cloud can receive per second over a sustained period of time.
Peak log rate/Rate limit	The maximum number of logs that FortiAnalyzer Cloud can insert into the database per second when there is a log rate restriction.
Tokens	FortiAnalyzer Cloud includes tokens which are consumed to allow FortiAnalyzer Cloud to temporarily surpass the peak log rate. See Exceeding log rate limits on page 26.

The supported log rates included with your FortiAnalyzer Cloud subscription is determined by your per-logging-device entitlements and any add-on storage SKUs added to FortiAnalyzer Cloud. For more information, see Logging support and daily log limits on page 22.

This topic includes the following information:

Viewing log rates limits and tokens

You can view your supported log rates and tokens in the FortiAnalyzer Cloud CLI.

To view the sustained and peak rate limit:

1. Sign in to FortiAnalyzer Cloud.
2. Select your username in the toolbar, and click *CLI*.
3. Enter the following command:

```
get system loglimits
```

The *Peak Log Rate* and *Sustained Log Rate* is displayed for your FortiAnalyzer Cloud instance

```
GB/day               : 6
Peak Log Rate        : 156
Sustained Log Rate   : 104
```

To view token usage and dropped logs:

1. Sign in to FortiAnalyzer Cloud.
2. Select your username in the toolbar, and click *CLI*.
3. Enter the following command:

```
diag log ratelimit
```

FortiAnalyzer Cloud displays information about the rate limit, tokens, and dropped logs.

```
Log rate limiting info for database insert
==========================================
  Rate Limit: 156(log/sec)
      Tokens: current=570,958 max=13,478,400 refill-interval=60(sec) refill-due=37(sec)
Dropped Logs: last-minute=0 since-sys-up=0
```

`Rate Limit`	The maximum number of logs that FortiAnalyzer Cloud per second. This is the same as the *Peak Log Rate*.
`Tokens`	`current`: The number of tokens currently available. `max`: The maximum number of tokens available in a 24 hour period. `refill-Interval`: The amount of time between each token refill. `refill-due`: The amount of time remaining until the next token refill. When the `refill-due` amount reaches `0`, the tokens will be refilled.
`Dropped Logs`	`last-minute`: The number of logs dropped in the last minute. `since-sys-up`: The number of logs dropped since the system was started.

How tokens are calculated

FortiAnalyzer Cloud rate limit tokens are calculated as follows. The following examples use a rate limit of `156`. This rate limit will vary depending on your license.

- The total tokens available per day: `rate limit x 60 seconds x 60 minutes x 24 hours = max tokens`
  Example: `156 x 60 x 60 x 24 = 13,478,400`
- The initial available tokens that the system assigns (1 hour worth of tokens): `rate limit x 60 seconds x 60 minutes = initial tokens`
  Example: `156 x 60 x 60 = 561,600`
- The amount of token added at each refill: `rate limit x 60 seconds = token refill`
  Example: `156 x 60 = 9,360`

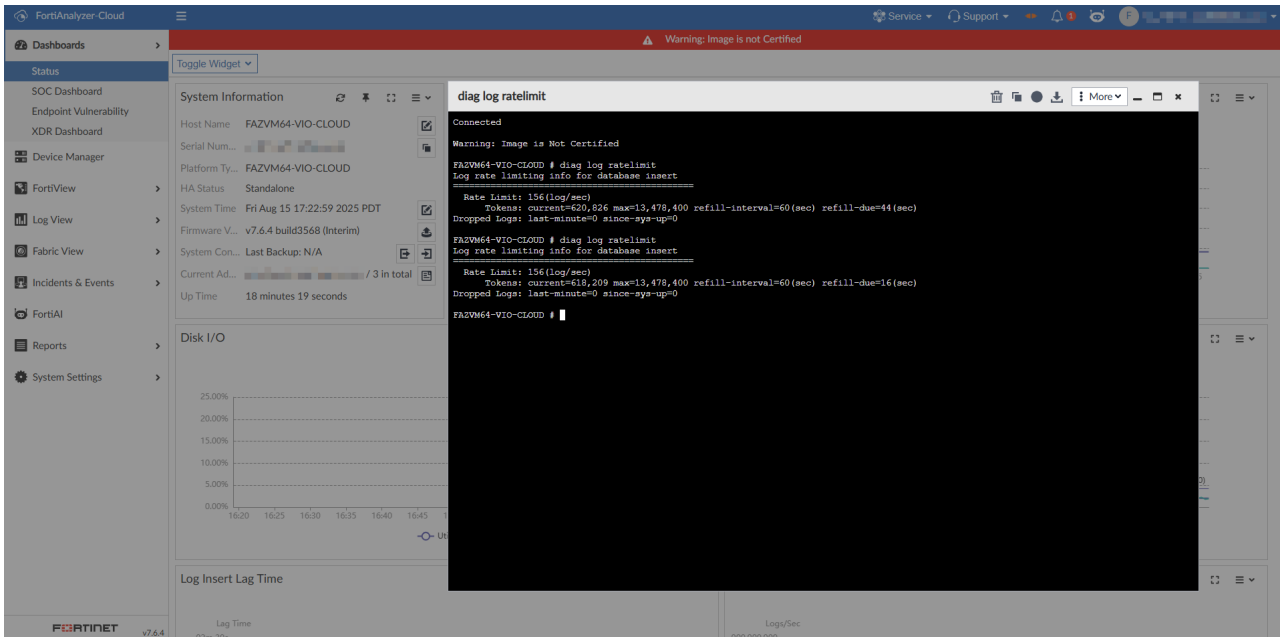
Exceeding log rate limits

FortiAnalyzer Cloud includes log rate tokens which are consumed to allow your FortiAnalyzer Cloud instance to temporarily surpass its peak log rate limit. This allows FortiAnalyzer Cloud to receive long logs or support short bursts of increased logging without dropping logs.

The number of tokens included with your FortiAnalyzer Cloud instance is determined based on your license, and are refilled each minute by a specified amount. See Viewing log rates limits and tokens on page 25.

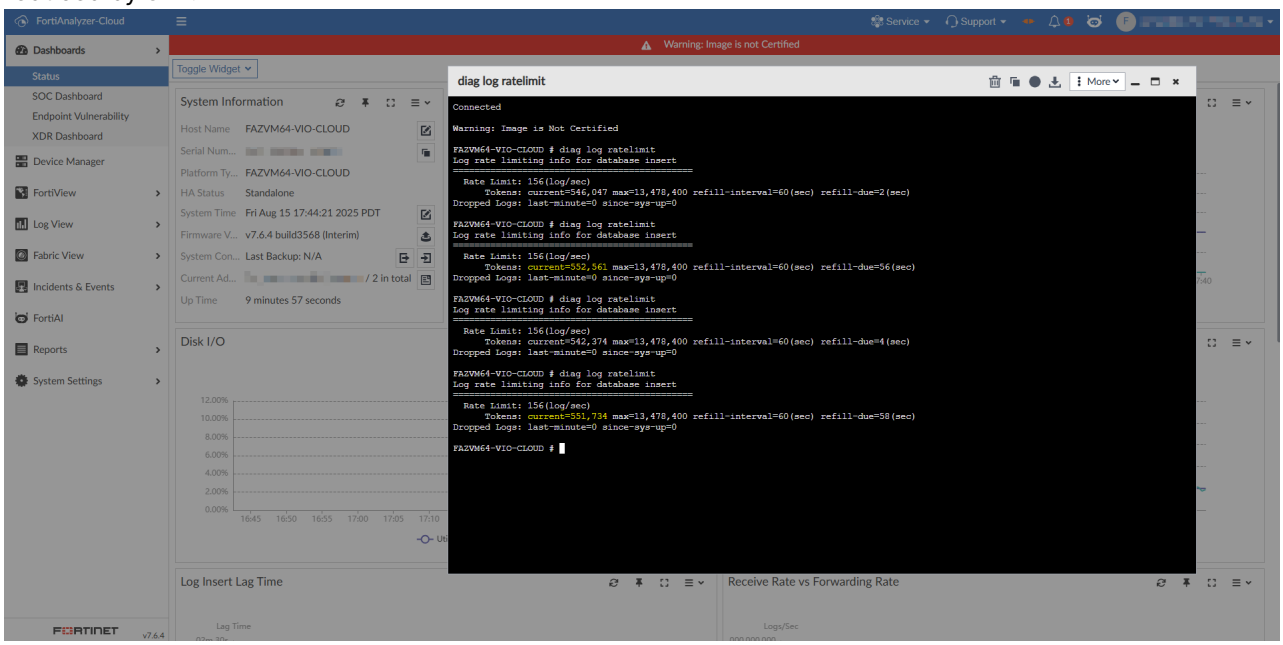
How tokens are consumed:

- Each log received by FortiAnalyzer Cloud that is greater than or equal to the log rate limit consumes one token.



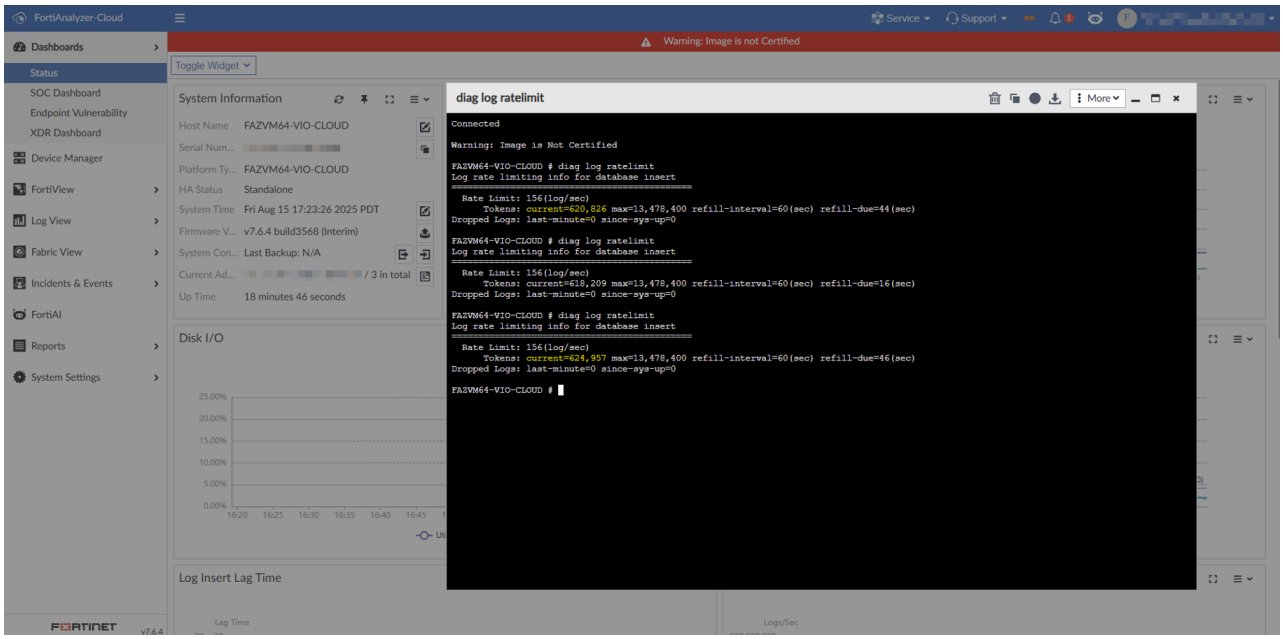
- When the received log rate is greater than or equal to the rate limit, the current token amount will be reduced as long as logs continue to arrive in FortiAnalyzer Cloud.

  In the following example, the *log receiving rate* is `200 logs /sec` which is greater than the *log rate limit* of `156 logs/sec`. When the token refill occurs after one minute, the number of available tokens has been reduced by 827.



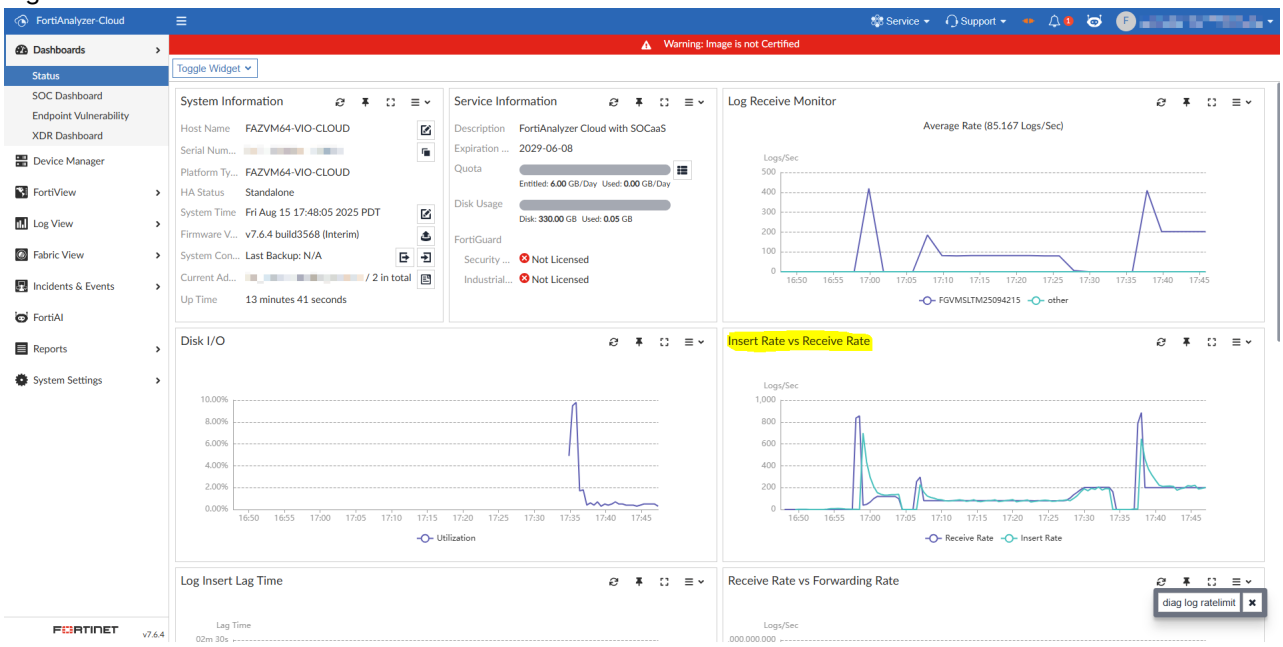
- When the received log rate is less than the rate limit, the token refill speed is faster than the consumption speed.

  In the following example, the *log receiving rate* is `80 logs/sec` which is less than the *log rate limit* of `156 logs/sec`. When the token refill occurs after one minute, the number of available tokens is increased by 4131.



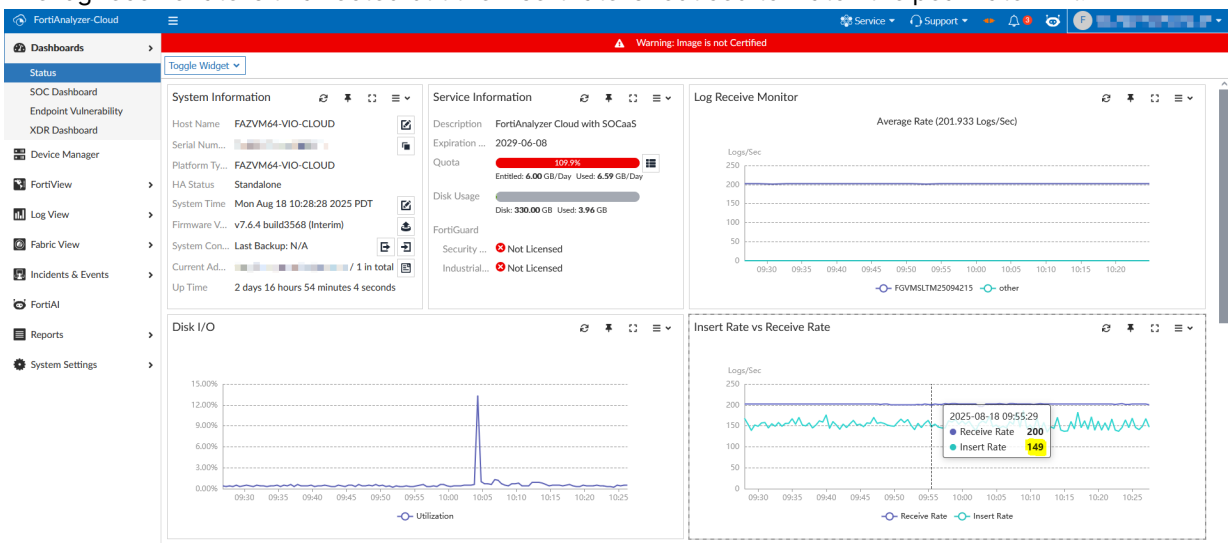
What occurs when all available tokens are consumed:

- When the number of remaining tokens is greater than the received log rate, tokens are consumed and the log's insert rate will match the receive rate.

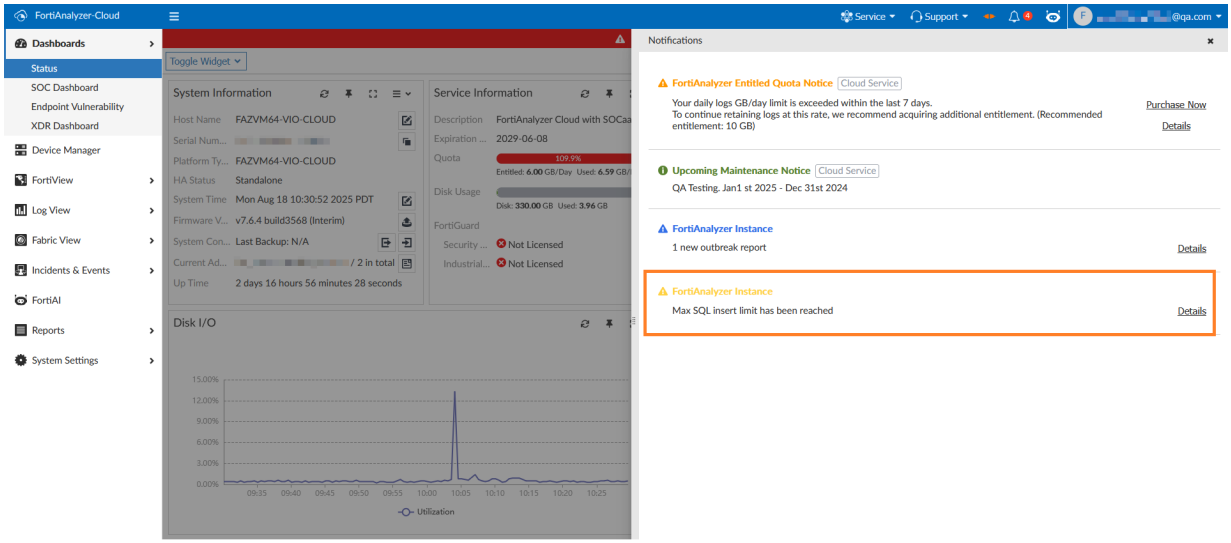


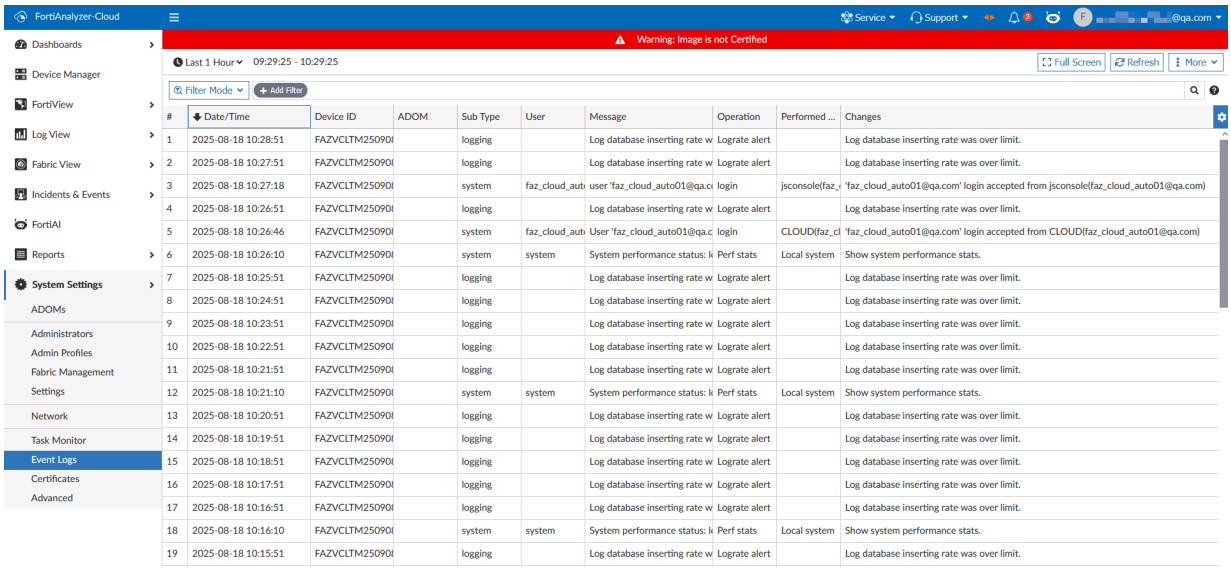
- When the log receiving rate surpasses the number of remaining tokens available, the following will occur:

- The log receive rate is unaffected but the insert rate is reduced to match the peak rate limit.



- Additional tokens will not be consumed to ensure the token amount does not drop below 0.
- Logs exceeding the rate limit are not inserted into the database.
- An alert is displayed in the notification drawer, and an event will be added to the event log with the message "*Log database inserting rate was over limit*" message.




FortiAnalyzer-Cloud
Service
Support
@qa.com
Warning: Image is not Certified
Dashboards
Device Manager
FortiView
Log View
Fabric View
Incidents & Events
FortiAI
Reports
System Settings
ADOMs
Administrators
Admin Profiles
Fabric Management
Settings
Network
Task Monitor
Event Logs
Certificates
Advanced
Last 1 Hour 09:29:25 - 10:29:25
Full Screen
Refresh
More
Filter Mode
Add Filter
Date/Time Device ID ADOM Sub Type User Message Operation Performed ... Changes
1 2025-08-18 10:28:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
2 2025-08-18 10:27:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
3 2025-08-18 10:27:18 FAZVCLTM250901 system faz_cloud_auto user 'faz_cloud_auto01@qa.c login jsconsole(faz_ 'faz_cloud_auto01@qa.com' login accepted from jsconsole(faz_cloud_auto01@qa.com)
4 2025-08-18 10:26:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
5 2025-08-18 10:26:46 FAZVCLTM250901 system faz_cloud_auto User 'faz_cloud_auto01@qa.c login CLOUD(faz_cl 'faz_cloud_auto01@qa.com' login accepted from CLOUD(faz_cloud_auto01@qa.com)
6 2025-08-18 10:26:10 FAZVCLTM250901 system system System performance status: l Perf stats Local system Show system performance stats.
7 2025-08-18 10:25:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
8 2025-08-18 10:24:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
9 2025-08-18 10:23:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
10 2025-08-18 10:22:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
11 2025-08-18 10:21:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
12 2025-08-18 10:21:10 FAZVCLTM250901 system system System performance status: l Perf stats Local system Show system performance stats.
13 2025-08-18 10:20:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
14 2025-08-18 10:19:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
15 2025-08-18 10:18:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
16 2025-08-18 10:17:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
17 2025-08-18 10:16:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.
18 2025-08-18 10:16:10 FAZVCLTM250901 system system System performance status: l Perf stats Local system Show system performance stats.
19 2025-08-18 10:15:51 FAZVCLTM250901 logging Log database inserting rate w Lograte alert Log database inserting rate was over limit.

www.fortinet.com